

令和8年8月 24 日修正

集約型教育用校務サーバー再整備事業 仕様書

令和8年8月

守口市教育委員会

1. 概要

1.1. 件名

集約型教育用校務サーバー再整備事業

1.2. 背景と目的

令和3年5月に文部科学省「教育情報セキュリティポリシーに関するガイドライン」（以下、国ガイドライン）が改訂され、クラウド活用と、ネットワーク分離を必要としないアクセス制御による対策が示された。本市では、校務系及び学習系ネットワークはセンター集約型の構成となっているが、利便性向上とコスト削減のため、極力設備を持たず、セキュリティを強化した新たな教育情報ネットワークの実現をめざす。

本事業は、ICTを活用した校務をより一層推進できる環境を整備することを目的に、新たなICTネットワークの構築移行、運用管理業務を委託するものである。

1.3. 導入方針

本事業の実施にあたり、以下の項目に関する事項に留意すること。

1. ネットワーク分離を必要とせず、認証によるアクセス制御を前提とした、新たな教育情報ネットワークを実現する。
2. 教職員の柔軟な働き方のため、校務用PC1台で校務系ネットワーク及び学習系ネットワークに接続でき、安全に利用できる環境を整備する。将来的には学校外（自宅等）からの安全な利用も想定する。
3. 本業務におけるセキュリティ対策は、認証、端末、通信、データ保護、監査、保守運用及びインシデント対応に対して各対策の実現方法、運用方法を含めて一体的に設計すること。
4. アクセス制御は原則として認証及び認可に基づいて実施することとし、IPアドレスによる制御は、必要性が明確な対象に限定して適用すること。
5. 教職員の業務負担を軽減するため、クラウドベースでの構築及び他システムの導入を行い、働き方改革を推進する。
6. 端末管理については、Microsoft Intune、Active Directory（GPO・ログオンスク립ト等）、本仕様で定めるIT資産管理システムを併用し、機能ごとに役割分

担すること。いずれか**単独**のみによる実装は、本仕様の要件を満たさないものとする。

7. 電子黒板端末、図書館端末、PC 教室端末 (Mac) 等についても、AD・Intune・IT 資産管理の**併用**により管理すること。AD のみ、Intune/Entra ID のみ、いずれかへの全面依存のみを前提とする実装は不可とする。現行の AD 運用 (GPO・ログオンスクリプト等) を**併用の選択肢**として維持できる構成とすること。

1.4. 前提要件

1.4.1. 関係事業者との連携

構築に当たっては、以下の関係事業者と情報共有を密にし、相互の責任分界点で不明瞭な箇所が発生しないように努め、問題が発生した場合は受注者が主体的に問題解決を図ること。

- ・ 必要に応じて問い合わせをすること。
- ・ 既存事業者にて作業が必要な際は、必要な費用を取得すること。

関係事業者

事業者	連絡先	主な関連業務
株式会社内田洋行 大阪支店 教育 ICT 事業部	TEL:06-6920-2641	既存ネットワーク・端末保守等

1.4.2. 庁外施設の統合への対応

本市の出先機関については、保守期間中に施設の統合により対象拠点数が変動する見通しである (1.9.実施場所 参照)。受託者は、対象拠点数が変わる可能性があることを前提として設計及び構築を行うこと。

- ・ 受託者は、保守期間中に当該変動が生じた場合に、機器の再配置、流用、予備機活用その他必要な対応を円滑に実施できるよう、機器選定、設置条件、設定方針、監視方式、台帳整備及び成果物作成において十分配慮すること。

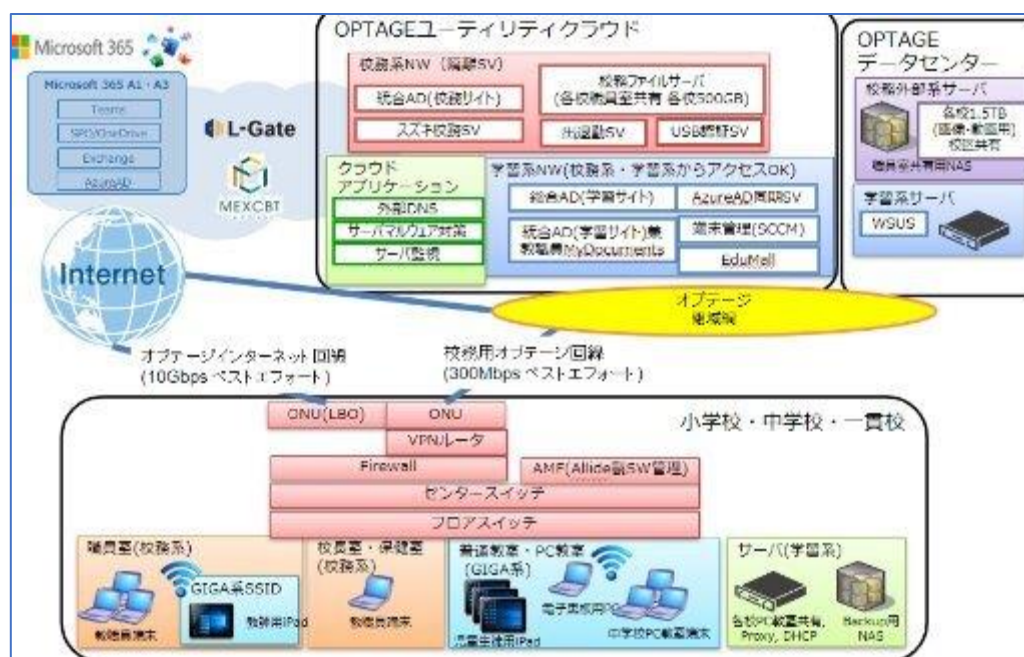
- ・ 拠点廃止等により不要となった機器については、将来的に必要なに応じて他拠点へ転用又は予備機として活用できるよう、設定初期化手順、再設定手順、移設時の確認事項及び管理方法を整理し、成果物に反映すること。

1.5. 全体構成

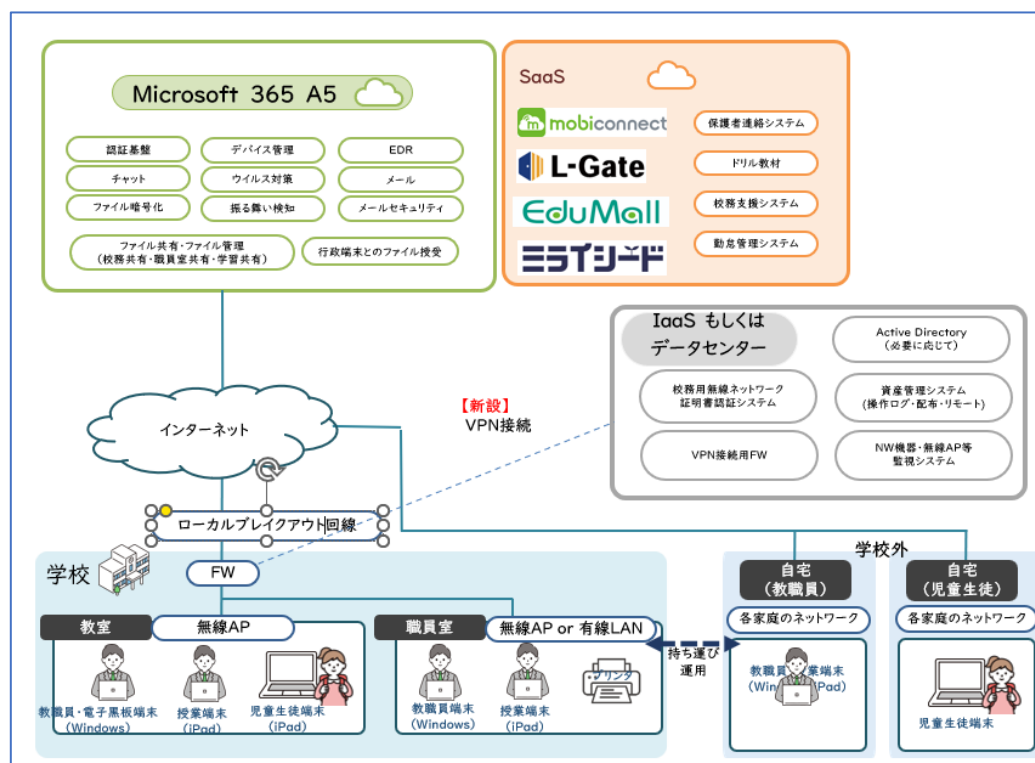
1.5.1. 構成の基本方針

本業務で想定する全体構成の概念を以下に示す。

【現状構成図】



【想定する全体構成概念図】



- クラウド化を前提とし、校務系の主要業務基盤はクラウドサービス(Microsoft 365 A5)による構成とする。
- 認証・セキュリティ基盤(RADIUS/電子証明書配布、IT 資産管理、ネットワーク監視等)は、国内データセンターまたは同等の IaaS 環境上に構築することを基本とする。本仕様の機能要件を満たす場合は、クラウド SaaS 型も可とする。
- 各学校(及び教育委員会事務局)から上記基盤への接続は、拠点間 VPN 等の安全な接続を構成すること。VPN と同等のセキュリティレベルを別方式で実現する場合は、設計書にて根拠を明示すること。
- クラウドサービス(Microsoft 365 等)へのアクセス経路として、GIGA スクール構想にて整備済のインターネット回線(学校個別接続、最大 10Gbps ベストエフォート)を利用する。本回線の整備は本業務の範囲外とする。
- 教育委員会事務局のインターネット回線は必須である。なお、現在、10Gbps 回線は設置されておらず、300Mbps 回線を使用している。

1.5.2. 現行からの変更概要

項目	現行	新システム
ネットワーク	学習系・校務外部接続系・校務系の3分離	統合（認証によるアクセス制御）
校務ファイル	OPTAGE ユーティリティクラウド・DC NAS	SharePoint Online / OneDrive
校内サーバー	DHCP・Proxy 等	データセンター/IaaS 基盤またはクラウド代替へ移行
校務系閉域回線	利用中	移行完了後廃止予定（回線統合）
端末制御 （教職員端末）	Active Directory GPO・ログ オンスクリプト	Intune + IT 資産管理 + AD （移行期間併用可）
端末制御 （電子黒板等）	Active Directory GPO・ログ オンスクリプト	AD・Intune・IT 資産管理の併用 （単一手段依存不可）

1.5.3. 継続利用システム

以下は調達範囲外であるものの、構築後も利用できることを前提とする。

No.	システム名	備考
1	校務用 PC (963 台 + 予備)	カメラ搭載
2	教職員用 iPad (854 台)	授業運用、既存 MDM (MobiConnect) 継続
3	電子黒板用端末 (553 台)	AD・Intune・IT 資産管理の併用 (2027 年リプレイスまで)
4	学習 e ポータル (L-Gate)	SSO 連携・アカウント管理・ダッシュボード
5	デジタル教科書配信 (Edumall)	
6	デジタル採点 (Answer Box Creator)	ローカル環境のみでの運用
7	保護者連絡 (COCOO)	グローバル IP 使用
8	学習系フィルタリング (i-FILTER@Cloud)	
9	給食献立管理システム	

廃止・移行対象(本業務で対応)

- 各校校内サーバー(DHCP・Proxy)
- 校務ファイルサーバー・職員室共有 NAS
- Backup 用 NAS(データ移行支援)
- 外部 DNS(移管・再構築)
- OPTAGE ユーティリティクラウド上の校務系基盤(移行後廃止)

1.6. 導入範囲

本業務の調達範囲は、国ガイドラインを念頭に置いたセキュリティ強化のため、以下の内容を含む。

- クラウドサービス(Microsoft 365 A5)の構築・設定
- データセンター/IaaS 上の基盤システム(後述 4 章)の構築
- **Active Directory(AD)基盤の構築・移行(GPO・LDAP 連携等、併用管理の選択肢として)**
- 連携ソフトウェアの導入、機器設定、動作確認
- 校内ネットワーク機器の設定変更(ハードウェア更改は範囲外)
- クライアント端末の設定変更
- データ移行
- 試験運用、利用者研修
- プロジェクト管理、要件定義、基本設計、詳細設計
- 5 年間の運用保守
- **学習 e ポータル(L-Gate)との SSO 連携、アカウント管理、学習ドリルダッシュボード機能**

規模要件

項目	要件
稼働時間	24 時間 365 日(計画保守を除く)
利用者数	教職員 963 名 全ユーザーの同時利用でパフォーマンス低下がない構成
児童生徒数	小学校 6,098 人、中学校 2,678 人(令和 8 年度 5 月時点)

1.7. スケジュール(案)

時期	内容
令和 8 年 8 月～9 月前半	キックオフ・設計
令和 8 年 9 月後半～	構築
令和 8 年 12 月～令和 9 年 1 月	教職員端末切替 (電子黒板端末は対象外。1 月以降に再設定)
令和 9 年 4 月 1 日	本稼働

※構築テストの時期は教育委員会と協議の上、決定

契約期間

- ・ 構築期間: 契約締結日から令和 9 年 3 月 31 日まで
- ・ 運用保守期間: 令和 9 年 4 月 1 日から令和 14 年 3 月 31 日まで(60 か月)

1.8. 契約・支払

- ・ 契約方法: リース契約(または提案に応じ教育委員会と協議)
- ・ 支払方法: 構築費は、構築が完了次第、一括払いとする。運用保守費は、月末日締め翌月支払いの月払いとする。
- ・ Microsoft 365 A5 ライセンス費用(教職員 963 ライセンス+運用に必要な管理者分)は構築期間中を含め本契約に含めること
- ・ 構築期間中のソフトウェアライセンス費用は事業者負担とする
- ・ 運用期間中の利用リソース・通信量増加による追加請求は不可とする

1.9. 実施場所

期間(予定)	場所
契約締結日 ～令和 10 年 6 月 30 日	小学校 12 校、中学校 7 校、さつき学園、教育委員会事務局(計 21 拠点)
令和 10 年 7 月 1 日～ 令和 14 年 3 月 31 日	小学校 11 校、中学校 6 校、さつき学園、八雲学園(八雲中学校区義務教育学校)、教育委員会事務局(計 20 拠点)

拠点増減の一時費用は別途契約ただし、設置・撤去についての調整を実施すること。
また回線使用料等、拠点数が減ることにより減額となる費用が生じる場合は、変更契約し減額すること。

2. システム要件

2.1. クラウド基盤システム

クラウド基盤システムは **Microsoft 365 A5** による導入を行うものとする。以下のサービスについて構築・導入すること。

(ア)クラウドセキュリティ

Microsoft 365 A5 に含まれるセキュリティ機能(Defender 系、Purview 系、Entra ID P2 等)を活用し、ゼロトラスト型のアクセス制御を実現すること。

(イ)認証基盤(IDaaS)

Microsoft Entra ID(旧 Azure AD) をクラウド型 ID 管理基盤として採用し、以下を実現すること。

要件	内容
一元管理	ユーザーID・認証情報の一元管理
SSO	メール・ファイル・コミュニケーションツール等への統合アクセス
多要素認証	ID・パスワードに加え追加要素による認証。利用場所・端末状態・リスクレベルに応じた動的制御
リスクベース認証	Identity Protection による不正サインイン検知・自動制御
SAML 連携	連携可能なシステムについて SSO を実現
管理職区分	管理職ユーザと一般教職員ユーザの区別管理。管理職のみアクセス可能なデータ領域・暗号化権限
端末認証	教職員端末起動時の BitLocker PIN+Windows Hello for Business による多要素認証(端末搭載カメラによる顔認証可能)

Application Proxy	テレワーク等における安全なアプリケーション公開
-------------------	-------------------------

ログインユーザー制御(想定)

端末種別	制御方式	ログイン
教職員端末 (Windows)	Intune + IT 資産管理 (AD は移行期間併用可)	M365 (教職員)
教職員 iPad	Entra ID + 既存 MDM (MobiConnect)	M365 (ASM ユーザー)
電子黒板端末 (Windows)	AD・Intune・IT 資産管理の併用	ローカルユーザー (ログイン後 M365 アプリからログイン)
図書館・PC 教室 (Mac)	AD・Intune・IT 資産管理の併用	AD またはローカル (現行踏襲)

(ウ)メール

Exchange Online により教職員・児童生徒向けメール環境を提供すること。Microsoft Defender for Office 365 によるフィッシング・マルウェア・なりすまし対策、添付ファイル・URL 事前検査を実施すること。

(エ)ファイル管理

OneDrive for Business / SharePoint Online により個人用・組織共有用ファイル管理を実現すること。アクセス権限・共有範囲の制御、操作履歴・アクセスログ、バージョン履歴管理を実施すること。

ファイルストレージ構成 (SharePoint)

- ・ 個人用: OneDrive (教職員 1 人 1 アカウント)
- ・ 学校保存領域: 学校ごとの SharePoint サイト (エクスプローラー類似のドキュメントフォルダ構成)
- ・ 共有保存領域: 教育委員会・全市教職員向け 1 サイト
- ・ 人事異動に伴うアクセス権の自動付与・削除 (Entra ID 連携)
- ・ 重要サイトへの接続元 IP アドレス制限

(オ)コミュニケーションツール

Microsoft Teams によるチャット、オンライン会議、ファイル共有。会議参加者制御、待機室、画面共有制限等のセキュリティ機能を設定すること。

- ・ チーム作成:教職員不可(管理者のみ)。チャンネル作成:教職員可
- ・ 学校ごとにチームを作成
- ・ 匿名ユーザ参加時はロビー待機

(カ)フィルタリング(校務系)

※学習系は i-FILTER@Cloud 利用中のため本調達範囲外。校務系は M365 A5 のサービスで運用設計を実施すること。

- ・ 不正・危険な通信の検知・遮断
- ・ クラウドアプリ利用状況の可視化・ポリシー制御
- ・ 異常アクセス・振る舞い検知時の自動アクセス制限

(キ)ウイルス対策・EDR

Microsoft Defender for Endpoint により端末上のマルウェア検知・振る舞い検知・封じ込め・復旧を実現すること。メール・ID・クラウドアプリとの統合脅威対応を実施すること。

(ク)ファイル暗号化・DLP

Microsoft Purview Information Protection により情報保護ラベルを設定すること。

No.	秘密度ラベル	暗号化	ガイドライン対応
1	最高機密	あり	I
2	高機密	あり	II
3	機密	あり	III(新規 Office ファイルの既定ラベル)
4	公開	なし	IV

- ・ 手動ラベル付け・自動ラベル付けポリシーを設定
- ・ エンドポイント DLP・Exchange DLP を設定(USB コピー、印刷、クリップボード、未許可サイトアップロード等を制御)
- ・ 校務共有データへの自動暗号化ラベル設計(管理職・一般・教務等)

(ケ)デバイス管理(Intune の範囲)

Microsoft Intune により、M365 連携に必要な端末管理を実施すること。対象端末および適用機能は第 3 章の併用設計に従い、A 区分を主とし、B 区分についても併用の一手段として利用可とする。本項の範囲を超える操作統制・ログ取得・資産管理は、第 5 章の IT 資産管理システムで実施する。

項目	Intune で実施する内容
デバイス登録	教職員 Windows 端末の Entra ID/Intune 登録
Windows Update	先行配信グループ・本番配信グループの 2 段階配信 (0～30 日差)
アプリ配信	サイレントインストール対応アプリの配信
基本セキュリティ	Windows ファイアウォール、BitLocker、Bluetooth 制御
コンプライアンス	ポリシー非準拠端末のアクセス制限
構成プロファイル	M365 利用に必要な端末設定

Intune では実施しないもの (IT 資産管理システムで実施)

- ・ 操作ログ・ファイル操作ログ・Web アクセスログの詳細取得
- ・ USB デバイスのシリアル単位管理・持ち込み検知
- ・ ソフトウェア配布のキャッシュ配信・帯域制御
- ・ 複数端末の一斉遠隔操作・画面一覧監視
- ・ IT 資産インベントリの詳細検索・台帳管理
- ・ IP アドレス管理台帳との照合

2.2. 構築環境の仕様(データセンター/IaaS)

セキュリティ強化を目的として調達する IaaS またはデータセンター上のシステムについて、以下の環境要件を満たすこと。なお、パブリッククラウド (Azure、AWS など) を利用する場合、日本国内リージョンで同等の要件を満たしている場合に限り、可とする。

1. **立地**: 日本国内。異ルートアクセス可能。水害・津波対策。免震構造 (応答加速度 250gal 以内)
2. **建物・設備**: 防火区画、ガス消火設備、JDCC Tier4 相当の電源、無停電電源、自家発電 (24 時間稼働可)
3. **空調**: 24 時間 365 日、16～27℃

4. **セキュリティ**:24 時間 365 日入退室管理、生体認証または有人警備
5. **通信回線**:複数事業者から選択可。2 回線入線時は異なる局舎・ルート

サーバーリソース(参考要件)

項目	要件
CPU	Xeon 6520P 相当以上(24 コア以上)
メモリ	128GB 以上
ストレージ	実効容量 9.6TB 以上(RAID5)。2 倍以上のバックアップ媒体
冗長化	リスクヘッジのため冗長構成

※為替リスク等による契約期間中の値上げ交渉は不可

2.3. 学習 e ポータル(L-Gate)連携

本市では、全小中学校で学習 e ポータル(L-Gate)を継続利用する。本項に定める**アカウント管理**および**ダッシュボード機能**を調達のすること。構築時の初期設定から運用期間(60 か月)全体を通じ、本契約の範囲に含めること。

2.3.1. 連携の基本方針

項目	要件
対象システム	学習 e ポータル(L-Gate)
認証基盤	Microsoft Entra ID との SSO 連携
連携対象 アカウント	教職員、児童生徒、ミライシードアカウント
費用	L-Gate 事業者への連携設定・年次更新・問い合わせ等に必要な費用を本契約に含める
責任分界	L-Gate 本体の機能改修は L-Gate 事業者、Entra ID 側設定・連携運用・ダッシュボード構築は受注者

2.3.2. アカウント管理

(ア)SSO 連携(構築時)

- ・ 既存システムで利用中の L-Gate と Microsoft Entra ID をアカウント連携 (SSO) すること。
- ・ SAML 等の連携方式は L-Gate 事業者と協議の上、設計書にて確定すること。
- ・ 教職員・児童生徒が L-Gate および Microsoft 365 へ同一 ID 体系でアクセスできること。
- ・ 構築完了時点で、L-Gate 経由の SSO ログインおよび Microsoft 365 へのシングルサインオンが動作することをシステムテストで確認すること。

(イ) 年次更新(運用時・毎年度必須)

以下の年次更新業務を、運用期間中毎年度実施すること。

1. 教職員・児童生徒の Microsoft 365 アカウントの年次更新
2. ミライシードアカウントの年次更新
3. L-Gate と Entra ID のアカウント連携 (SSO) を維持したままの更新

年次更新の運用フロー(基本)

1. 年度末に本市から教職員人事情報 (Excel) を受領する
2. 受領データを CSV 等に変換し、L-Gate へ取り込む
3. L-Gate から Entra ID へユーザ同期を行う
4. Entra ID へ所属学校情報が反映されない場合は、本市から受領した人事情報をもとに、各教職員ユーザへ所属学校属性を付与する
5. L-Gate の年次更新実施後、Microsoft 365 についても自動更新される運用とする

年次更新の期限

- ・ 年度末の更新対象開示から年度内に作業を完了すること
- ・ 新学期開始時に新アカウントで利用開始できること

その他

- ・ L-Gate 管理画面用の管理者アカウントは本市から払い出す
- ・ 年次更新以外の日次アカウント更新は本市が実施 (受注者の対応範囲外)
- ・ 運用期間中に L-Gate 事業者への問い合わせ・調整が必要な場合、その費用を本契約に含める

(ウ)アカウント管理の運用代行

教育委員会・教育センターからの依頼に基づき、以下を実施可能とすること。

- ・ L-Gate と Entra ID 間の SSO 連携設定・証明書管理
- ・ 年次更新作業の代行(上記フローに基づく)
- ・ L-Gate 事業者との連携調整

2.3.3. 学習ドリルダッシュボード機能

別途本市が選定・指定する学習ドリルについて、既存 L-Gate 上にダッシュボード機能を構築し、運用期間(60 か月)を通じて利用可能とすること。本機能の構築費用・ライセンス費用・保守費用を本契約に含めること。対象となる学習ドリルの名称等は、入札参加申請を行った事業者へ開示する。

機能要件

No.	要件	内容
1	学習状況の可視化	データに基づく児童生徒の学習状況把握を目的に、利活用状況を可視化できること
2	ログ取得	活用ログの取得が個人・校園(学校)・委員会単位で可能であること
3	ダッシュボード管理	ダッシュボード表示データの追加・削除・変更が可能であること
4	利用期間	本稼働日(令和 9 年 4 月 1 日)から運用期間満了まで継続利用可能であること
5	権限管理	学校管理者・教育委員会管理者等、役割に応じた表示範囲の制御が可能であること

構築・テスト要件

- ・ 構築期間中に L-Gate 事業者と連携し、ダッシュボード機能の設計・構築・設定を完了すること
- ・ 指定学習ドリルからのデータ連携方式(API、ログ連携等)を設計書に記載すること
- ・ システム導入テストにおいて、個人・学校・委員会単位での表示およびログ取得を確認すること
- ・ 操作マニュアル・管理者向け設定手順書を納品すること

2.3.4. 本項不適合とする仕様

以下に該当する仕様は、本仕様の必須要件を満たさないものとする。

- L-Gate との SSO 連携・年次更新を本市または L-Gate 事業者のみの対応とし、受注者の業務範囲外とするもの
- ダッシュボード機能を別契約・別調達とするもの
- Power BI 等、L-Gate 外のツールのみで代替し、L-Gate 上のダッシュボードを構築しないもの
- 構築のみ、または 1 年間のみ等、60 か月の運用を含まないもの

3. 端末管理・IT 資産管理の役割分担

入札の公平性および本市の運用実態を踏まえ、端末管理は **Active Directory・Microsoft Intune・IT 資産管理システム**を併用し、機能ごとに役割分担する。

機能領域	Microsoft Intune	Active Directory	IT 資産管理システム(第 5 章)
Entra ID/Intune 登録	○	—	—
ドメイン参加・GPO	△(B 区分等で併用可)	○(併用可)	—
ログオンスクリプト	—	○(併用可)	—
Windows Update 配信	○	△(GPO/WSUS 等と併用可)	—
M365 アプリ配信	○	△	△(大容量・キャッシュ配信)
BitLocker ポリシ	○	○(GPO と併用可)	○(回復キー収集・管理)
—			
USB 書き込み制御	○	○(GPO と併用可)	○(シリアル単位の詳細制御)
操作・ファイル・Web ログ	—	—	○(必須)

インベントリ・資産 台帳	△	—	○(必須)
遠隔操作・画面監 視	△	—	○
ソフトウェア配布 (キャッシュ)	○	△(GPO/ログオンスクリ プトと併用可)	○
ローカルデータ保 存禁止等	○(DLP 連携)	○(GPO と併用可)	○(操作ログと 併用)

※同一機能を AD と Intune の両方で重複設定しないこと。併用設計書で管轄を明示すること。

設計要件

- 端末種別ごとに、AD・Intune・IT 資産管理の併用方針および機能別の管轄を設計書に明記すること。
- IT 資産管理システムは、全 Windows 端末(教職員端末・電子黒板等を含む)に導入すること。
- AD の GPO・ログオンスクリプトと Intune 構成プロファイルを併用する場合、設定の競合・重複が生じないように設計すること。
- 教職員端末・勤怠打刻端末については、USB 書き込み制御・ローカルデータ保存禁止等のセキュリティ設定を新環境でも設計・適用すること(必要性を含め協議)。

3.1. 端末種別の管理構成(ハイブリッド管理)

本市では、端末の特性に応じて AD・Intune・IT 資産管理を併用する。全端末の単一手段への統一(AD のみ／Intune のみ)を前提とする仕様は不可とする。

管理区分	対象端末	併用の基本方針
A:教職員 端末	教職員端末(校務)、勤怠打 刻端末	Intune + IT 資産管理を主とし、移行 期間中は AD(GPO 等)との併用可
B:共用・ 特殊端末	電子黒板、図書館、PC 教室 (Mac 仮想)、メディアセンタ ー	AD + IT 資産管理を基本とし、Intune は端末・機能に応じて併用可

C:MDM 管理	教職員 iPad、児童生徒用 iPad	Entra ID + MobiConnect
-------------	------------------------	------------------------

B 区分端末の併用設計の考え方

- ・ 現行の AD (GPO・ログオンスクリプト) による運用実績があり、AD を併用の選択肢として維持できること
- ・ 同時に、Intune で設定可能な項目 (Windows Update、一部セキュリティポリシー等) は併用してよい
- ・ 個人 M365 アカウントでのログオンが困難な端末でも、IT 資産管理による操作統制・ログ取得は必須
- ・ 2027 年リプレイス予定の電子黒板等について、段階的に Intune 適用範囲を拡大する設計も可

3.2. AD・Intune・IT 資産管理の併用設計

3.2.1. 基本方針

- ・ 端末管理は AD 依存ではない。AD・Intune・IT 資産管理を組み合わせ、端末種別・機能ごとに最適な併用構成を設計すること。
- ・ データセンター/IaaS 上に Active Directory を構築し、GPO・ログオンスクリプト・LDAP 連携を併用の選択肢として利用可能とすること。AD 廃止のみ、または AD 単独のみの仕様は不可とする。
- ・ Entra ID (クラウド ID) と AD は共存させ、必要に応じ Entra Connect 等によるハイブリッド ID 連携を設計すること。
- ・ 設計書には、端末種別×管理機能マトリクス (どの機能を AD/Intune/IT 資産管理のどれが担うか) を必ず添付すること。

3.2.2. 併用設計で満たすべき機能 (端末種別を問わず)

以下の機能は、AD・Intune・IT 資産管理の併用により実現すること。単一手段のみは不可とする。

機能	要件
端末環境設定	GPO、Intune 構成プロファイル、ログオンスクリプト等の併用で実現

セキュリティ設定	USB 制御、暗号化、ファイアウォール等を適切な手段で設定(競合しないこと)
資産・操作管理	IT 資産管理によるインベントリ、操作ログ、USB 管理、遠隔操作(全 Windows 端末で必須)
ドメイン参加	AD 併用端末はドメイン参加を維持可能とすること
RADIUS/LDAP 連携	無線認証等で AD/LDAP 参照が可能であること
M365 利用	教職員端末は Entra ID/Intune、電子黒板等は端末特性に応じた併用設計

3.2.3. 端末種別の移行・併用要件

端末	台数	併用設計の要点
教職員端末(校務)	963 台	Intune+IT 資産管理を主。AD から段階的移行可。統合 AD からの離脱可
勤怠打刻端末	21 台	同上
電子黒板用端末	553 台	AD(GPO 等)+IT 資産管理を基本。Intune 併用可。Office 2024 インストール
図書館端末	21 台	AD+IT 資産管理の併用。Intune 併用可
PC 教室(Mac 仮想)	147 台	AD 参加維持+IT 資産管理。学習共有クラウド化に伴う設定変更
メディアセンター端末	1 台	AD+IT 資産管理の併用

- ・ マスタ PC によるイメージ展開方式も可とする
- ・ 教職員端末と B 区分端末では、AD 離脱の要否が異なる場合がある。設計書で方針を明示すること
- ・ 学校現場で教職員が実施する端末初期設定(複合機・プリンタ設定等)の範囲は、現行踏襲または併用設計に基づき再設計すること

3.2.4. 本項不適合とする仕様

- ・ AD のみ、Intune のみ、IT 資産管理のみのいずれか単独で全機能をまかなうもの
- ・ 電子黒板等について、AD(GPO・ログオンスクリプト)を併用の選択肢として提供しないもの
- ・ 全端末の Entra ID/Intune への全面移行のみを前提とし、現行 AD 運用の併用余地を認めないもの
- ・ AD と Intune で同一設定を重複適用し、競合対策を設計書に示さないもの

4. セキュリティ強化(基盤システム)

本案件にて調達する IaaS もしくはデータセンター上に、以下のシステムを実装すること。それぞれ単一のシステムとして調達し、複数製品の組み合わせによる実現は認めない。ただし、各システムが SaaS 型であり、本仕様の機能要件を満たす場合は採用可能とする。

4.1. 校内ネットワーク機器監視システム

要件	内容
監視対象	ネットワーク機器等の CPU・メモリ・ディスク使用率
可視化	一覧画面・グラフ表示
閾値監視	設定値超過時の異常検知
通知	障害発生・復旧時のメール等による自動通知

4.2. 無線接続用電子証明書配布システム

カテゴリ	要件
管理画面	日本語・英語対応。暗号化アクセス。RADIUS/CA/LDAP/ネットワーク状態表示
仮想化	VMware ESXi、Nutanix AHV、Hyper-V 上で動作可能
RADIUS	5,000 アカウント以上。パスワード有効期限・変更禁止期間。MAC アドレス認証(PAP/CHAP)
冗長	複製構成。利用者グループ単位の複製
ログ	NAS-Identifier、NAS-IP-Address、送信元 IP。EAP-TLS 時の証明書情報
EAP-TLS	クラウド CA 連携によるクライアント・サーバー証明書認証
DHCP	複数ネットワーク対応。リース数 5,120 以上
クラウド型	構築も可

4.3. IT 資産管理システム

第 5 章に定める機能要件を満たす専用システムとする。Microsoft Intune のみでは代替不可。

4.4. 外部 DNS

ドメイン「edu-moriguchi.jp」のゾーン情報を管理する DNS サーバーを提供すること。既設保守事業者からの管理権限移管、切替後の継続利用確認を実施すること。利用料を含むこと。

4.5. DHCP サーバー

各校の校内サーバー廃止に伴い、DHCP 機能を移行すること。実装方式は以下のいずれかとする。

- **方式 A(データセンター/IaaS 集中型)**: データセンター/IaaS 上のシステムで各校ネットワークに IP 配布(VPN 経由等)
- **方式 B(拠点アプライアンス型)**: 各校にアプライアンス型 DHCP サーバーを設置(冗長 2 台/拠点)

いずれの方式も以下を満たすこと。

- 配布対象: 校務用 PC、電子黒板用 PC、教職員用 iPad、児童生徒用 iPad
- リース数: 2,500 以上(方式 A の場合は全体で 5,120 以上)
- 設定バックアップ(手動・自動)
- クラウド管理コンソールからの設定管理(方式による)

4.6. Active Directory(AD) 基盤

AD・Intune・IT 資産管理の併用のため、データセンター/IaaS 上に Active Directory ドメインサービスを構築すること。AD は端末管理の**唯一の手段**ではなく、GPO・ログオンスクリプト・LDAP 連携等の併用選択肢として提供する。

要件	内容
ドメインサービス	Windows Server Active Directory。現行校務系統合 AD に相当するドメイン設計
ドメイン参加	各学校から VPN 等経由でドメイン参加・GPO 適用が可能であること
GPO	端末環境設定、セキュリティ設定、ソフトウェア制限等を GPO で配信できること
ログオンスクリプト	現行運用のログオンスクリプトを移行・継続利用できること
冗長化	ドメインコントローラーは冗長構成とすること
Entra ID 連携	教職員 M365 利用のため、必要に応じ Entra Connect 等によるハイブリッド ID 連携を設計すること
LDAP 連携	無線接続用電子証明書配布システム等から LDAP 参照が可能であること

5. IT 資産管理システム(機能要件)

以下の機能要件をすべて満たすシステムを調達すること。

5.1. 基本要件

- ・ ISMS(ISO27001)およびプライバシーマークを取得しているメーカーの製品
- ・ 保守期間中はマイナー/メジャー/後継品を問わず最新版を提供
- ・ ISO/IEC20000 認定メーカーのサポート体制
- ・ 全機能を一つのインストーラーで提供
- ・ クライアント操作画面の管理端末での一覧表示

5.2. IT 資産管理(インベントリ)

- ・ 自動収集・検索: 各クライアントのハードウェア情報、ソフトウェアインストール状況、OS バージョン、空き容量、死活監視状態などを自動収集し、一覧表示・検索できること。

- 詳細検索: AND/OR/NOT 検索、キーワード(空白区切りによる複数指定)、数値範囲指定が可能であること。
- 検索条件管理: 検索条件ごとに表示項目の順序や表示・非表示を定義・保存し、呼び出せること。
- 削除端末の管理: システムから削除されたクライアントコンピューターも検索対象に指定できること。
- BitLocker 管理: BitLocker 等の回復キーを収集・管理し、暗号化状態を一覧表示できること。回復キーは CSV 形式でエクスポート可能であり、状態変更時はドライブログとして記録すること。
- ソフトウェア配布: 任意指定端末やグループに対し、プログラムの実行・解除を一括で行えること。
- キャッシュ配布: 同一セグメント内のキャッシュ端末を活用した配信、通信帯域制限、同時接続数制限が可能であり、4GB 以上のファイル配布に対応すること。
- 資産照合: IP アドレス管理台帳と資産情報を照合し、競合、不正使用、使用期限切れを一覧またはマップ形式で表示できること。
- ネットワーク機器通知: セグメント内で最後にシャットダウンする端末に対し、稼働中のネットワーク機器情報をポップアップ通知すること。

5.3. デバイス管理(USB 等)

- 台帳管理: USB デバイスのシリアル・ベンダーID を自動収集し、個体識別による管理台帳を作成・一覧表示すること。
- 使用制限: 指定した USB デバイスに対し、ネットワーク全体や部署、ユーザー、端末の組み合わせ単位で、使用許可/不許可/書き込み禁止を柔軟に設定できること。
- 紛失防止: 所定期間使用実績のない USB デバイスを紛失の可能性ありと自動判定し、所在確認を促す通知を行うこと。
- 所持者特定: 装着日時とログオンユーザー情報を紐づけ、現在の所持可能性が高いユーザーを自動的に特定して表示すること。
- 履歴参照: USB メモリ最終使用時のファイル一覧表示、および当該ファイルに対する操作履歴を抽出表示できること。
- 不正持込判定: システム外で作成・編集された外部ファイルの持ち込みを自動判定し、その USB デバイスの使用を禁止すること。

5.4. リモート操作

- ・ 遠隔操作: ネットワーク経由でリモート操作が可能であり、管理機のログオンパスワードを変更できること。
- ・ 複数端末監視: 複数端末の画面を静止画で同時に確認(順次更新)でき、操作対象を切り替えられること。
- ・ 画面隠蔽操作: セキュリティの観点から、クライアント側の画面を隠しながら遠隔操作(Windows 8 以降対応)ができること。
- ・ 操作支援: ファイル転送、クリップボード共有(テキスト・画像)、通信量の自動コントロール、一斉キー・マウス操作(操作ロック・センタリング等)が行えること。
- ・ 通知: リモート操作中にクライアント側へポップアップ通知を表示すること。

5.5. 運用要件

- ・ 手順化: ソフトウェア配布および Windows Update(Intune 連携・スケジュール配信)について、本市担当者が実施可能な手順書を提供すること。

6. 接続時対策

各学校からの安全な接続のため、以下を実施すること。

要件	内容
ファイアウォール	FortiGate と同等の機能を有する機器(仮想アプライアンス可)
拠点間 VPN	データセンター/IaaS 上の FW と各校 FortiGate 間で構成
ユーザー数	ユーザー数に依存しない VPN 利用
認証連携	Active Directory、RADIUS 等との連携、二要素認証対応
仮想化対応	VMware、KVM、Hyper-V、AWS、Azure 等
代替	VPN と同等のセキュリティレベルを実現する場合、VPN 構築は不要(設計書に根拠を明示)

ネットワーク移行に伴う校内設定変更

- 各校ネットワーク機器(FW、センタースイッチ、フロアスイッチ、無線 AP):ハードウェア現行利用、設定変更のみ
 - 校務系閉域回線廃止に伴う回線統合・FW ポリシー変更
 - 802.1x 認証導入に伴う機器・無線 AP 設定変更
 - 校内サーバーDHCP・Proxy 機能の移行
-

7. セキュリティポリシー策定支援

- 国ガイドライン(令和 6 年 1 月版以降)に準拠
 - 「教育委員会情報セキュリティポリシー対策方針」「対策基準」の策定
 - ガイドラインハンドブック、総務省ガイドラインにも準拠
 - 各学校への説明・研修、自己点検、ポリシー見直し(1 回)の費用を含む
-

8. 構築業務要件

8.1. 基本要件

- 守口市情報セキュリティポリシー指針に従うこと
- 5 年間運用可能なシステムを選定
- 導入時最新バージョンを原則導入
- 既存機器への設定変更費用を含む
- 構築のために別途、管理用ライセンスが必要な場合は事業者で費用を負担
- 運用環境とは別途、テスト環境を用意する場合は事業者で費用を負担

8.2. プロジェクト体制

- ・ プロジェクト体制表の作成にあたっては、プロジェクトマネージャー、作業責任者等、関係者の役割、連絡先を明確にすること
- ・ プロジェクトマネージャーはシステム設計・構築・運用業務を5年以上行った経験を有すること
- ・ プロジェクトマネージャー及び作業責任者がマイクロソフト法人向けユニファイドサポート契約による支援を受けられるようにすること
- ・ 以下の各条件を満たす者をプロジェクトメンバーに含めること(保守運用実績と構築実績をそれぞれ別のメンバーで満たすことも可とする)

項目	条件
保守運用実績	本市と人口が同等規模以上の自治体において Microsoft 365 A5 での保守運用実績を有する
構築実績	本市と人口が同等規模以上の自治体において Microsoft 365 A5 でのゼロトラストモデルを構築完了した実績を有する

8.3. プロジェクト管理

- ・ 定例会議(月1回以上)での進捗報告
- ・ 議事録の速やかな提出
- ・ 仕様・要件の確認は書面により実施
- ・ 課題管理表の毎回確認

8.4. 要件定義・設計

- ・ ネットワーク設計(物理・論理)
- ・ システム設計(基本・詳細・セキュリティ・移行・運用)
- ・ 配線・電波利用調査(必要時、費用含む)
- ・ 設計ドキュメントの納品

8.5. システム導入テスト

- 本番環境でのテスト実施
- バックアップ・リストアテスト(協議の上)
- アクセス制御・データ分類・情報漏洩対策の動作確認
- L-Gate と Entra ID の SSO 連携、年次更新フローの動作確認
- 学習ドリルダッシュボードの表示・ログ取得(個人・学校・委員会単位)の動作確認
- テスト環境は別途用意する場合、事業者負担

8.6. クライアント端末設定変更

端末種別ごとの併用設計は第 3.1 章・第 3.2 章に従うこと。設計書には端末種別 × 管理機能マトリクスを添付すること。

端末種別	台数	管理区分	併用設計の要点
教職員端末(校務)	963 台	A	Intune+IT 資産管理を主。AD は移行期間併用可。統合 AD からの離脱可
勤怠打刻端末	21 台	A	同上
電子黒板用端末	553 台	B	AD+IT 資産管理を基本。Intune 併用可。Office 2024 インストール
中学校 PC 教室 (Mac 仮想)	147 台	B	AD+IT 資産管理。学習共有のクラウド化に伴う設定変更
児童生徒用 GIGA 端末 (iPad)	—	C	MobiConnect
教員用授業端末 (iPad)	—	C	同上
図書館端末	21 台	B	AD+IT 資産管理の併用。Intune 併用可
メディアセンター端末	1 台	B	同上

併用設計の共通要件

- 全 Windows 端末に IT 資産管理エージェントを導入すること
- AD(GPO・ログオンスクリプト)と Intune を併用する場合、設定競合を回避すること

- 端末種別ごとに、どの機能を AD/Intune/IT 資産管理のどれが担うか設計書に明記すること
- マスタ PC によるイメージ展開方式も可とする

テスト確認事項

- 各端末種別:併用設計通りの設定適用、IT 資産管理エージェント動作
- AD 併用端末:ドメイン参加、GPO/ログオンスクリプト動作
- Intune 併用端末:登録・コンプライアンス動作
- AD と Intune 併用端末:設定競合がないこと

8.7. 成果物

プロジェクト計画書、体制図、課題管理表、要件定義書、ネットワーク構成図、配線図、基本設計書、詳細設計書、テスト結果報告書、運用設計書、操作研修計画書、操作マニュアル、議事録、セキュリティポリシー案、**端末管理併用設計書(端末種別×AD/Intune/IT 資産管理マトリクス)**、**Active Directory 設計書**、**L-Gate 連携設計書(SSO・年次更新フロー)**、**学習ドリルダッシュボード設計書・操作マニュアル** 等

9. 移行・切替

9.1. データ移行

現行の共有構成と同等の領域を構成し、データ移行を実施すること。

移行対象(主要)

共有種別	現行	移行先
校務共有	UC/各校 500GB+教育委員会 11TB	SharePoint Online
職員室共有	DC NAS/各校 2TB(計 34TB)	SharePoint Online
学習共有	各校サーバー/各校 2TB	SharePoint Online 等

- 暗号化ファイルは復号して移行
- フォルダ構成・アクセス権は現行と同等を設計

- ・ 365 ラベリング設計(校務共有への自動暗号化、役職ラベル)
- ・ データ抽出は受注者が実施(ログイン情報は本市提供)

9.2. 既存 365 ライセンス移行

現行 A3 ライセンスから A5 へ最適タイミングで順次移行

9.3. 切替スケジュール

- ・ 教職員端末:12 月～1 月(電子黒板は 1 月以降)
- ・ パイロット校:11 月(ユーティリティクラウド・SharePoint 両方アクセス可能な状態で検証)

10. 運用・保守要件

10.1. 運用統括

- ・ 運用統括者の設置、定期報告、継続的改善提案
- ・ 定例会:1 年目月 1 回、2 年目以降 3 か月ごと(年 4 回)

10.2. ヘルプデスク

項目	内容
電話受付	平日 8:30～17:30
メール/FAX	24 時間 365 日受付(対応は翌営業日以降可)
窓口	M365・本調達システム・端末修理等を一元対応(複数窓口不可)
現地対応	必要時は派遣
記録	全件蓄積・保管・定例報告

- ヘルプデスクにおいて、L-Gate の SSO ログイン障害、年次更新に関する問い合わせを一元受付すること
- L-Gate 本体の不具合については L-Gate 事業者へエスカレーションする手順を整備すること

10.3. システム等保守

- 障害対応、設定変更支援(協議の上)
- M365 システム監視・異常時保守
- Active Directory 基盤(GPO・ログオンスクリプト等)および AD/Intune 併用端末の保守・障害対応
- 端末種別ごとの併用設計に基づく GPO・Intune 構成プロファイルの更新支援
- 障害時のオンサイト保守(構築メンバー、同一会社内代理可)

10.4.ログ管理

IT 資産管理システム等により、以下のログをインシデント発生時の調査に利用可能な粒度(利用者、日時、接続元、対象機能、操作内容等を識別可能)で記録・検索・保管すること。

- 端末操作ログ: ログオン/オフ、ソフトウェア起動・操作時間、ファイル操作、共有フォルダアクセス、Web アクセス(閲覧・書き込み・アップロード)、クリップボード(テキスト・画像)、印刷ログ(ドキュメント名、枚数、パス)を記録すること。
- 詳細なファイル追跡: ファイル操作(作成、コピー、名変、移動、上書き、削除)をフルパスで記録すること。Office 製品の「名前を付けて保存」等の時系列追跡が可能であること。
- 通信・接続ログ: USB メモリ等のシリアル情報を含む利用状況、通信デバイス接続、指定範囲外 IP への TCP 通信(http/ブラウザ以外含む)を記録すること。
- クラウド連携: Microsoft 365 / Office Online 利用時のローカルファイル作成パスを記録すること。
- 管理・監査ログ: 管理者操作ログ、設定変更ログ、障害発生ログ、端末管理ログ、およびセキュリティ上重要なイベントログを取得し、発注者が確認可能であること。

- 自動バックアップ機能: 収集したログを一定期間ごとに自動でバックアップする機能を有すること。
- ログの保全: 端末側に一時保存されるログデータは、改変防止のため難読化されていること。

なお、管理にあたっては以下の要件をすべて満たすこと。

- 保存期間: 取得したすべてのログおよび監査証跡は、5 年間のリース期間すべてにわたり欠損なく保存すること。
- バックアップ運用: システムによる自動バックアップに加え、3 か月に 1 回手動取得し、指定のバックアップストレージへ保存すること。
- 対象範囲: 端末操作ログに加え、M365 関連アクセスログ(サインイン・Web フィルタリング・Teams)を網羅すること。
- 参照方法: バックアップされた過去のログについても、リストア(復元)作業を行うことなく、直近のログと同様に管理コンソール上で即座に検索・閲覧できること。
- 外部出力: 管理コンソールで抽出したログは、CSV 等の汎用的な形式で外部出力(エクスポート)可能であること。

10.5. SOC 業務(セキュリティ監視)

以下の SOC 業務を実施すること。

業務	内容	対応時間
EDR 監視	常時監視、高危険度アラート時の端末隔離	監視・隔離: 24/365
アラート分析	分析・報告・遮断解除	平日 9～17 時
Web 参照ログ調査	SWG 等での通信追跡	平日 9～17 時
DLP ログ調査	Purview ログ追跡	平日 9～17 時
M365 遠隔監視	専従担当者による監視(営業・構築者不可)	平日 9～17 時

10.6. 運用代行業務

教育委員会・教育センターからの依頼に基づき、以下を実施可能とすること。

- BitLocker 回復キー管理、MFA リセット
- SSO 連携・証明書管理
- Windows パッチ配信制御
- アプリケーション配信
- 外部記憶媒体の利用登録
- リモートワイプ
- Intune 構成プロファイル変更
- 操作ログ取得
- Web アクセス管理(ホワイトリスト等)
- SharePoint/Teams/site 権限管理
- 端末キッティング用アカウント払出
- L-Gate 年次更新作業の代行
- L-Gate SSO 連携・証明書の設定変更
- AD/Intune 併用端末向け GPO・Intune 構成プロファイルの設定変更

10.7. 研修会

対象	内容	回数
システム管理者	年次更新業務、管理ポータル、L-Gate SSO・ダッシュボード管理	導入後 1 回程度
管理職・情報担当・一般職員	利用方法、問合せ方法	導入後 1 回程度
各校教職員	端末操作、M365 アプリ、初期設定	各校 1 回、2 時間程度

- 研修動画・マニュアル作成を含む
- 会場・端末は教育委員会が準備

11 疑義

本仕様書の定めのない事項または疑義が生じた事項については、教育委員会と受注者が協議して定める。